Abstract

A system and method is directed to detecting tampering of a computer system's operating system (OS). The OS includes a kernel binary and at least one user level binary. When the user level binary is generated, selected integrity data is also generated. Such integrity data may include, but is not limited to, a digital signature, a hash associated with the user level binary, and the like. In one embodiment, integrity data is also generated for the kernel. The kernel is modified to include the integrity data associated with the user level binary. The kernel further includes a tamper detector that is configured to examine the OS binary against its associated integrity data. If tampering is detected, the tamper detector may provide a message indicating which OS binary may have been modified. The tamper detector may also quarantine the modified OS binary, log the message, and the like.